In the claims:

1. (currently amended) A method for re-establishing secure communications between a node and an endpoint node including the steps of:

copying, responsive to a reset at the node, a set of security associations stored in a memory to a working set of security associations, wherein the set of security associations includes only the security associations for a set of trusted endpoint nodes, the set of trusted endpoint nodes determined according to a security association re-use policy of the node , wherein the security association re-use policy controls the set of trusted endpoints to comprise ~~fewer than all of the endpoints that securely communicate with the node~~ only end-points that are well known to the node and communicate with the node on a regular basis;

receiving, at the node, a communication from the endpoint node;

determining whether a security association for the endpoint node is included in the working set of security associations;

responsive to a determination that the security association for the endpoint node is in the working set of security associations, using the security association to process the communication from the endpoint node.

2. (original) The method of claim 1, further including the step of verifying if the communication from the endpoint node is valid.

3. (original) The method of claim 2, further including the steps of:

obtaining a new security association for the endpoint node responsive to a determination that the communication from the endpoint node is not valid; and

storing the new security association for the endpoint node in the working set of security associations.

4. (original) The method of claim 1, further including the steps of:

obtaining a new security association for the endpoint node responsive to a determination that the security association for the endpoint node is not included in the working set of security associations; and

storing the new security association for the endpoint node in the working set of security associations.

5. (currently amended) A method of re-establishing communication between a node and an endpoint including the steps of:

selectively storing an identifier of the endpoint on a trusted endpoint list according to a re-use policy of the node, wherein the security association re-use policy limits the selection of identifiers for inclusion into the trusted endpoint list to ~~less than all of the endpoints that securely communicate with the node~~ only end-points that are well known to the node and communicate with the node on a regular basis;

negotiating a security association for the endpoint, and storing the security association for the endpoint in a working table of security associations; and

periodically copying a subset of the working table of security associations to a table of security associations in a memory, wherein the subset of the working table of security associations that is copied to memory is selected according to the trusted endpoint list.

6. (original) The method of claim 5, further comprising the step of:

in the event of a reset, copying the table of security associations to the working table of security associations.

7. (currently amended) A network device including:

security association logic, coupled to the non-volatile memory, for applying security associations to communications received by the network device, the security association logic including:

a first memory comprising at least one entry, the entry comprising an endpoint identifier for each endpoint communicating with the network device and a security association associated with the each endpoint; and

a list of trusted endpoints, the list of trusted endpoints being determined according to a security association re-use policy of the network device, wherein the security association re-use policy limits the inclusion of end-points in the trusted end-point list to ~~less than all of the endpoints that securely communicate with the network device~~ only end-point nodes that are well known to the node and communicate with the node on a regular basis; and

a second memory, storing a subset of data of the first memory, the subset of data selected according to the list of trusted endpoints.

8. (original) The network device of claim 7, wherein the second memory is a non-volatile memory.

9. (original) The network device of claim 7, further comprising means for periodically copying the subset of data of the first memory to the second memory.

10. (original) The network device of claim 9, wherein the subset of data from the first memory that is copied to the second memory is selected responsive to the list of trusted endpoints.

11. (original) The network device of claim 10 wherein only the entries of the first memory having endpoint identifiers that are on the list of trusted endpoints are copied to the second memory.

12. (original) The network device of claim 7, further comprising means, responsive to a reset at the network device, for copying contents of the second memory to the first memory.

13. (cancelled)

14. (previously presented) The method according to claim 1 wherein the security association re-use policy varies in response to network traffic.

15. (previously presented) The method of claim 1 wherein the security association re-use policy always selects identifiers associated fixed end points for inclusion in the trusted endpoint list.

16. (cancelled)

17. (previously presented) The method of claim 1 wherein the security association re-use policy varies in response to network traffic.

18. (cancelled)

19. (previously presented) The network device of claim 7 wherein the security association re-use policy varies in response to network traffic.

20. (previously presented) The network device of claim 7 wherein the security association re-use policy includes end-points that request trusted status.